# Quantum Information Science

*R. J. Hughes, D. J. Berkeland, G. L. Morgan, J. E. Nordholt, and C. G. Peterson (P-23)*

## Introduction

The representation of information by classical physical quantities such as the voltage levels in a microprocessor is familiar to everyone. But over the past decade, quantum information science has been developed to describe binary information in the form of two-state quantum systems, such as photon polarization states. (A single bit of information in this form has come to be known as a "qubit.") Remarkable new capabilities in the world of information security have been predicted that make use of quantum-mechanical superpositions of information, a concept that has no counterpart in conventional information science. For example, quantum cryptography allows two parties to communicate securely even in the presence of hostile monitoring by a third party. A quantum computer would make use of logical operations between many qubits and would be able to perform many operations in parallel. Certain classically intractable problems, such as factoring large integers, could be solved efficiently on a quantum computer. We have experimental projects underway in quantum cryptography, quantum computation, and in quantum optics with trapped strontium ions.

## Quantum Cryptography

One of the main goals of cryptography is for two parties ("Alice" and "Bob") to render their (binary) communications unintelligible to a third party ("Eve"). This can be accomplished if Alice and Bob both possess a secret random-bit sequence, known as a cryptographic key. For example, in "one-time pad" encryption Alice adds the key to the original message, known as plaintext, and communicates the sum (ciphertext) to Bob. He is able to recover the plaintext by subtracting his key from the ciphertext, but Eve, who is assumed to have monitored the transmitted ciphertext, is unable to discern the underlying plaintext through the randomization introduced with Alice's key. So, although key material conveys no useful information itself, it is a very valuable commodity, and methods for Alice and Bob to generate key material securely are correspondingly important.

Using quantum cryptography, or, more accurately, quantum key distribution (QKD), Alice and Bob can create shared cryptographic key material whose security is assured by the laws of quantum mechanics. They first independently generate secret random-number sequences, which then undergo a bit-wise comparison that requires the preparation, transmission, and measurement of a single photon for each bit. Alice's photon-state preparations and Bob's measurements are determined by their bit values and are chosen from sets of nonorthogonal possibilities, such as linear and circular polarization. This comparison algorithm, which may be publicly known, ensures that Bob detects a photon (with some quantum-mechanically determined probability) only if he has the same bit value as Alice. They retain only the detected bits from their initial sequences. These subsets are the raw key material from which a pure key is distilled using classical error-detection techniques. Eve can neither "tap" the key transmissions (owing to the indivisibility of a photon) nor copy them (owing to the quantum "no-cloning" theorem). Furthermore, the nonorthogonal nature of the quantum states ensures that if Eve makes her own measurements, she will be detected through the elevated error rate arising from the irreversible "collapse of the wave function" that she introduces.

QKD offers many security and ease-of-use advantages over existing key-distribution methods. Traditional key distribution using trusted couriers requires cumbersome security procedures for preparing, transporting, and handling the key before any communications can take place and may even be impractical (*e.g.*, rekeying a satellite). In contrast, quantum keys do not even exist before the QKD transmissions are made, and a key can be generated at message transmission time. Public-key cryptography also avoids many of the difficulties of key distribution by courier but provides only the conditional security of intractable mathematical problems, such as integer factorization. Accurate assessment of an adversary's computing power over the useful lifetime of encrypted information, which may be measured in years or even decades, is notoriously difficult: unanticipated advances in fields such as quantum computation could render public-key methods not just insecure in the future but also retroactively vulnerable. QKD could be used for real-time key generation in cryptographic applications where this long-term risk is unacceptable.

The physical systems that can support QKD transmissions determine the potential uses of quantum cryptography. We have demonstrated that QKD is possible over multikilometer optical-fiber paths: the necessary quantum coherence of the QKD transmissions persists even outside the controlled environment of a physics laboratory. At the infrared wavelengths required, germanium or indium-gallium arsenide avalanche photodiodes can be persuaded to detect single photons but at the penalty of a high noise and, hence, a high error rate. Removing these errors reduces the amount of key material and limits transmission distances to 100 km or so. (Optical amplifiers cannot be used to extend this range because they cannot replicate the nonorthogonal quantum states used in QKD.)

## Quantum Cryptography: Recent Achievements

In our experiment we have demonstrated quantum cryptography over 48 km of optical fiber that had been installed for network applications between two LANL technical areas. Our system incorporates an encryption/decryption feature that allows us to use the quantum-key material to encrypt short text messages at the sending computer and decrypt them at the receiving computer. (See Figure 1.) This experiment shows that QKD could be used to generate cryptographic keys over "open" optical-fiber links between secure "islands," such as between different government agencies in the Washington, D.C., area.

In a separate experiment we are developing QKD for "free-space," line-of-sight communications, such as surface-to-aircraft, surface-to-satellite or satellite-to-satellite in low-earth orbits. We have designed, constructed, and tested a quantum cryptography system that

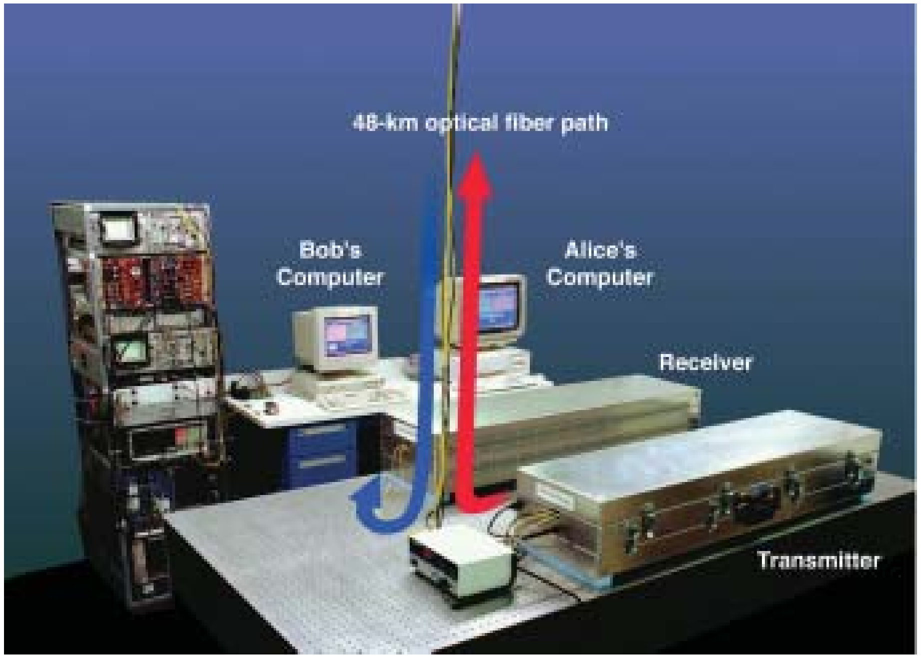

**Figure 1. The optical fiber quantum cryptography experiment**

creates and transmits—using single-photon transmissions—cryptographic random numbers between sending-and-receiving instruments that were separated by a 1.6-km outdoors optical path in daylight. The system is based on the propagation and detection of nonorthogonal polarization states of single photons in free space at a wavelength (772 nm) for which the atmosphere has a very low attenuation. We are now planning to extend the transmission range to more than 2 km and we are developing plans for a surface-to-satellite test experiment. Quantum cryptography is likely to be the first practical application of the foundations of quantum mechanics, which illustrates the often unexpected value of basic research.

## Quantum Computation

With two or more qubits it becomes possible to consider quantum logical-“gate” operations in which a controlled interaction between qubits produces a (coherent) change in the state of one qubit that is contingent upon the state of another. These gate operations are the building blocks of a quantum computer, which in principle is a very much more powerful device than any classical computer because the superposition principle allows an extraordinarily large number of computations to be performed simultaneously. In 1994 it was shown that this “quantum parallelism” could be used to efficiently find the prime factors of composite integers. Integer factorization and related problems that are computationally intractable with conventional computers are the basis for the security of modern public-key cryptosystems. However, a quantum computer running at desktop-PC speeds could break the keys of these cryptosystems in only seconds (as opposed to the months or years required with conventional computers). This single result has turned quantum computation from a strictly academic exercise into a subject whose practical feasibility must be urgently determined.

The architecture of a quantum computer is conceptually very similar to a conventional computer: multiqubit, or “multibit,” registers are used to input data; the contents of the registers undergo logical-gate operations to effect the desired computation under the control of an algorithm; and, finally, a result must be read out as the contents of a register. The principal obstacles to constructing a practical quantum computer are (1) the difficulty of engineering the quantum states required; (2) the phenomenon of “decoherence,” which is the propensity for these quantum states to lose their coherence properties through interactions with the environment; and (3) the quantum measurements required to read out the result of a quantum computation. The first proposals for practical quantum-computation hardware, based on various exotic technologies, suffered from one or more of these problems. However, in 1994 it was proposed that the basic logical-gate operations of quantum computation could be experimentally implemented with laser manipulations of cold, trapped ions: a qubit would comprise the ground (S) state (representing binary 0) and a suitably chosen metastable excited (D) state (to represent binary 1) of an ion isolated from the environment by the electromagnetic fields of a linear radio-frequency quadrupole ion trap.

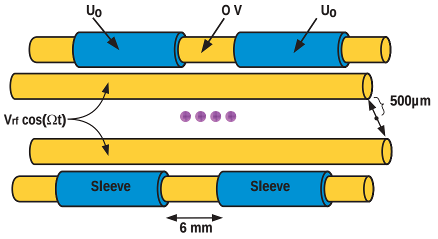

**Figure 2. A schematic diagram of the segmented linear Paul trap confining four ions along its axis.**

The principles of this proposed quantum computer can be illustrated with our trapped strontium ion project. We have recently confined strontium ions in a novel yet simple linear Paul trap with segmented electrodes, as depicted in Figure 2. A radio frequency (rf) potential $V_0$ Cos($\Omega t$), where $V_0 < 100$ V and $\Omega/2\pi = 7$ MHz, is applied to two diagonally opposite rods of the trap to confine the ions radially. To confine the ions axially, the outer segments of the remain ing two rods are connected to a potential $U_0$, typically between 5 and 50 V. Additional potentials can be applied to any of the electrodes and their segments to move the ions to the nodal line of the rf field, where perturbations to the ion motion from the rf field are minimized. Figure 3 shows an image of two ions confined in this trap.

Figure 4 shows a partial-energy-level diagram of $^{88}Sr^+$ and the optical transitions that are relevant to these experiments. The 422-nm $S_{1/2}\leftrightarrow P_{1/2}$ transition is used to Doppler-cool the ions. Approximately 7.5% of the decays from the $P_{1/2}$ state are to the metastable $D_{3/2}$ state. To optically pump the atomic population out of the $D_{3/2}$ state, resonant 1092-nm light from a multimode fiber laser drives the $D_{3/2}\leftrightarrow P_{1/2}$ transition. Finally, a diode laser emitting 674-nm light drives the narrow $S_{1/2}\leftrightarrow D_{5/2}$ transition. The metastable $D_{5/2}$ state and the $S_{1/2}$ ground state would be the qubits in the quantum-computation experiment.

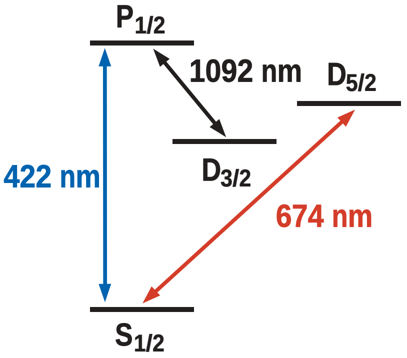

Figure 4. Relative energy levels and transitions of $Sr^+$.

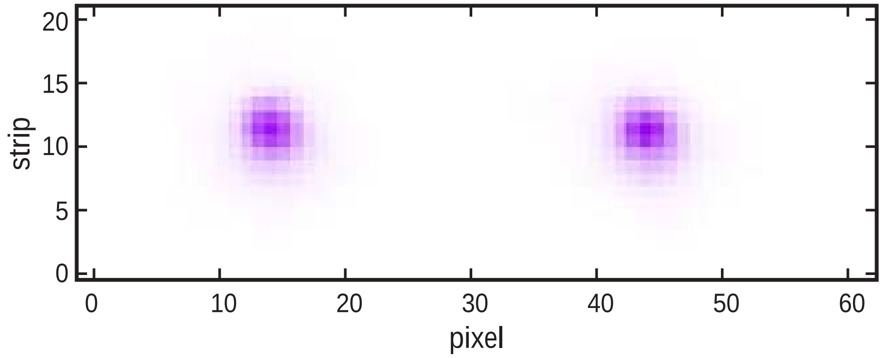

Figure 3. An image of two strontium ions approximately 20 μm apart.

By driving both the strong $S_{1/2}\leftrightarrow P_{1/2}$ and weak $S_{1/2}\leftrightarrow D_{5/2}$ transition in these ions, as depicted in Figure 5, we have observed quantum jumps[1] as shown in Figure 6. Here, the fluorescence from the broad $S_{1/2}\leftrightarrow P_{1/2}$ transition vanishes when the ion has been excited to the long-lived $D_{5/2}$ state and returns when the ion either decays out of the $D_{5/2}$ state or is laser-driven out of the $D_{5/2}$ state. According to quantum theory, the times at which the atom makes a transition to or from the $D_{5/2}$ state are random. As with other quantum-mechanical processes (such as scattering photons from a beam splitter into one of two ports), this can form the basis of a random number generator, which is of crucial importance to cryptological applications. Unlike in other quantum mechanical systems, however, a single ion undergoing quantum jumps can very cleanly test whether these quantum processes are truly random[2]. Previously, such tests have been made with relatively short and nonsequential strings of quantum jump data with single mercury ions[3]. We are in the progress of making such tests in one and several strontium ions, using data sequences long enough (≈$10^4$ jumps) to yield cryptographically significant results.

We can also perform spectroscopy on the $S_{1/2}\leftrightarrow D_{5/2}$ transition. For example, when the 674-nm diode laser's frequency is scanned over the resonance, we see a resonance curve as shown in Figure 7. Being able to control the ion as it makes the transition between these two states is a critical component in the development of an ion quantum logic gate, and we are further developing our apparatus to do this.

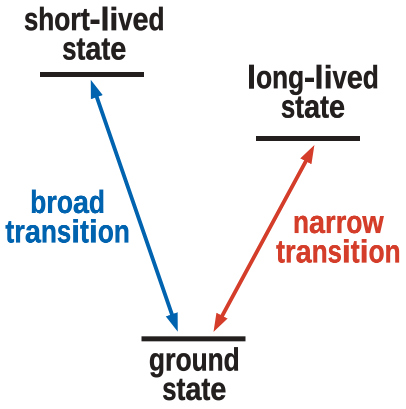

Figure 5. V-configuration for observing quantum jumps.

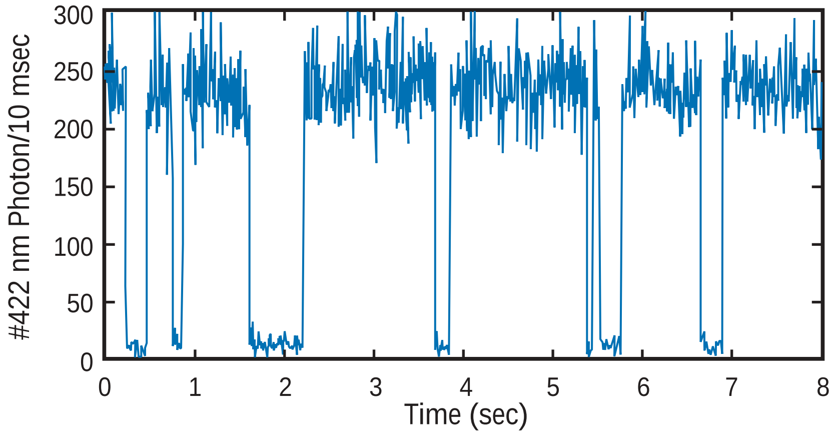

**Figure 6. Quantum jumps in $^{88}Sr^{+}$.**

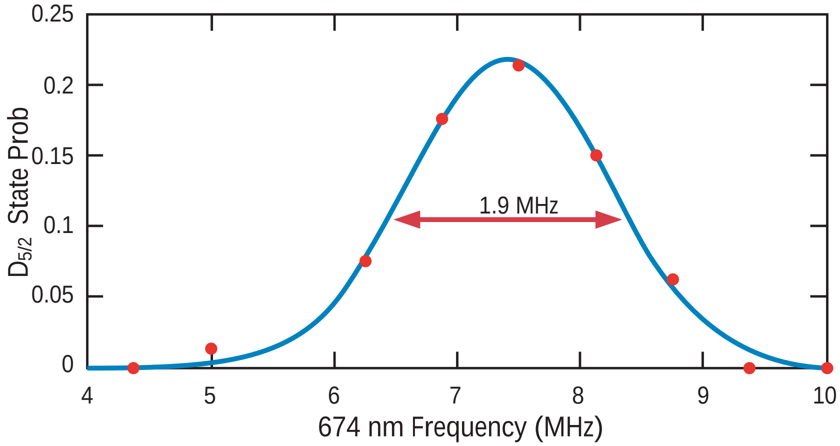

**Figure 7. A low-resolution spectrum of the $S_{1/2}$↔$D_{5/2}$ transition.**

## Contact Information

For further information about these projects please contact
Richard J. Hughes,
Physics Division, H803,
phone: (505) 667 3876
Los Alamos National Laboratory,
e-mail: hughes@lanl.gov
Los Alamos, NM 87545
http://p23.lanl.gov/Quantum/quantum.html

## References/Further Reading

[1] R. J. Cook, “Quantum Jumps,” in *Progress in Optics XXVIII*, E. Wolf, ed. (Elsevier B.V., 1990) pp. 362-416.

[2] T. Erber and S. Putterman, *Nature* 318, 41 (1985).

[3] T. Erber et al., *Ann. Phys.* (NY) 190, 254 (1989).